# 2013 Year-End Policy Review

**PO1001** **Information Security Policy**

**Target Audience**: All Users

**Summary**: The intent of this policy is to explain the range of acceptable and unacceptable uses of State-provided information technology (IT) resources

**Additions**: Wording around FTI modified to better meet IRS requirements.

**PO1002** **Acceptable Use of State-Provided Wireless Devices**

**Target Audience:** Any users that have or use state-issued mobile phones, tablets, laptops, or other similar devices.

**Summary:** This policy establishes a framework for the procurement, possession, and appropriate use of West Virginia state-owned and/or paid wireless communication equipment and/or services. In addition, all rules regarding the acceptable use of IT resources within State agencies apply to the utilization of portable devices.

**Additions:** Portable devices that can be connected to the network must be attached at least once every 14 days for a minimum of two hours and until all updates have been successfully loaded, to receive program updates, security patches, and anti-virus definition updates. FTI and PII should not be viewed on a portable device. If the employee cannot restrict confidential and/or sensitive information on the screen from public view, the portable device must not be used unless specifically authorized. Policy 1004, "Acceptable Use of Portable Devices" was consolidated into this policy.

**PO1005** **E-Mail Use Standards**

**Target Audience**: Any user that uses email and/or instant messenger.

**Summary**: This policy establishes and communicates the acceptable use of, access to, and disclosure of the State-provided e-mail system.

**Additions**: Agencies with access to FTI must have a procedure in place that articulates the protocols of using electronic mail for transmitting and receiving files containing FTI. FTI should not be transmitted or used on an agency's internal e-mail systems, unless absolutely required to complete a business function. FTI must not be transmitted outside of agency, either in the body of an e-mail or as an attachment. If transmittal of FTI within the agency's internal e-mail system is necessary, certain precautions must be taken.

**PO1006** **Data Classification**

**Target Audience**: Data Owners and Data Custodians

**Summary**: This policy presents the framework through which all State of West Virginia (State) government agencies, employees, vendors, and business associates, specifically those in the Executive Branch, must classify their data and systems, as they relate to (1) data sensitivity; and (2) data and system criticality

**Additions**: Lists Federal Tax Information (FTI) as Sensitive Information in the document examples

**PO1008** **Information Security Auditing Program**

**Target Audience**: State entities or personnel who are involved in IT audits

**Summary**: This policy explains the authority of the WVOT Information Security Audit Program, as well as the standards of WVOT audit practice.

**Additions**: Agency's audit reports and requests involving FTI must be maintained for five (5) years, or according to the applicable records control schedule, whichever is longer.

**PO1010** **Acceptable Use of State-Provided Instant Messaging**

**Target Audience**: All users who use instant messaging on State system

**Summary**: This policy Outline the applicable rules applied when using the State-provided system.

**Additions**: No sensitive information, including Federal Tax Information (FTI) and Personally Identifiable Information (PII) will may be shared through Instant Messaging.

**PO1011** **Media Protection**

**Target Audience**: All users

**Summary**: This policy defines standards, procedures, and restrictions for removable media that connects to any device or to a WVOT-supported network, in an order to store, back-up, relocate, or otherwise access enterprise

**Additions**: Employees are prohibited from using flash drives or portable media that do not have adequate protection mechanisms to store or transmit sensitive data (e.g., Protected Health Information, sensitive Personally Identifiable Information, Federal Tax Information (FTI)).

**PO1014** **Anti-Virus**

**Target Audience**: Technicians, management, end users

**Summary**: This policy describes prescribes the measures required to counter computer viruses and identifies responsibilities in protecting the State network against malicious software.

**Additions**: Any information system that stores, processes, or transmits Federal Tax Information (FTI), Personal Health Information (PHI), or Personal Identity Information (PII) must be protected against malicious code transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Malicious code protection mechanisms will be employed at critical

information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network where feasible.

**PO1017** **Use of Social Media**

**Target Audience: E**mployees, contractors, or vendors who utilize, review, monitor, and/or update social media sites as a function of their job within the State of West Virginia.

**Summary**: This document provides policy for appropriate implementation, responsible use, correct security measures, and professional conduct of internal and external social media (i.e. Facebook, Twitter, YouTube, Flickr, etc. ).

**Additions**: Only business related activities are sanctioned. Any user of Social Media for State purposes must be required to read and acknowledge the Social Media Policy signoff sheet. Any content used or disseminated on the Internet is limited to non-confidential and non-sensitive information. Users shall not post confidential, sensitive, legally protected, or proprietary information. Users are prohibited from using social networking sites from State equipment for political purposes, to conduct private commercial transactions, or to engage in other personal and private activities. Users who connect to Social Media web sites through State information assets, are subject to all agency and State requirements addressing prohibited or inappropriate behavior in the workplace, including acceptable use policies, user agreements, sexual harassment policies, internet usage policies, etc. Users will not visit any social media web sites that are not related to a business purpose. Users will exercise extreme caution while on social media sites and will not click unknown links; download unapproved programs; or put at risk any State system or network.

**PO1018** **Network Violation Reporting**

**Target Audience:** Agency and Department Management

**Summary:** This policy outlines the courses of action prescribed for both for agencies when network violations are detected on the State network.

**Additions:** On the third violation and creation of a Network Violation Report for a user, Internet access will immediately be suspended until Agency leaders and WVOT personnel meet and discuss actions to mitigate ongoing risk.

**PO1019** **Wireless Access Points**

**Target Audience**: All users that install, authorize, or recommend wireless points.

**Summary**: This document prescribes how wireless technologies will be deployed, administered, and supported to assure that State of West Virginia employees, guests, and contractors have access to a reliable, robust, and integrated wireless network, and to increase the security of the wireless network to the fullest extent possible.

**Additions**: Any unapproved access point discovered in operation, and located on State property, whether connected to the WVOT network or not, is subject to being disabled and removed immediately and indefinitely, by the WVOT. This includes but is not limited to personal cell phones being used as a WAP. Wireless Access Points should not be used in the flow of sensitive information (e.g. Federal Tax Information).

**PO1021** **Account Management**

**Target Audience:** Agency Approval Authorities

**Summary:** This policy outlines the standards for creating, issuing, removing, monitoring, and managing employee accounts.

**Additions:** Minor word edits, no substantial content changes.

**PO1022** **Internet Usage**

**Target Audience**: All Users

**Summary**: This policy explains the acceptable and unacceptable uses of State-provided internet access.

**Additions**: No Private Health Information (PHI), Personally Identifiable Information (PII), Federal Tax Information (FTI), or other sensitive material shall be placed on or made available via the Internet. Any transmission of confidential data that is required for business purposes must be preapproved and encrypted during transmission.

**PO1025** **Accreditation and Certification**

**Target Audience**:

**Summary**: This policy is outlines how the West Virginia Office of Technology (WVOT) validates the security readiness for devices, systems, application and system software, and other technology prior to deployment into a production status.

**Additions**: Whenever information systems contain Federal Tax Information (FTI), the agency must: a) Manage the information system using a life cycle methodology that includes information security considerations; and b) Obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.

**PO1026** **WVOT Monitoring Policy**

**Target Audience**: For use by agency personnel responsible for helping with IT audits.

**Summary**: The purpose of this document is to outline the West Virginia Office of Technology (WVOT) policy regarding the monitoring and logging of network traffic that traverses the WVOT Backbone. It does not affect end users but has been produced to aid in audits.

**Additions:** Minor word edits, no substantial content changes.